REMARKS

The Examiner has rejected Claims 1-21 under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The Examiner has also similarly rejected the specification on similar grounds. Specifically, the Examiner asserts that applicant's claimed technique "wherein an update of a key distribution center database of shared keys is, at least in part, capable of being avoided when at least one of the nodes is unfamiliar" has not been described in the specification.

In the latest Office Action dated 9/20/2005, the Examiner has argued that "*at most* [paragraphs 0005-0006] suggest or imply the claimed limitation." Specifically, the Examiner has stated that "the cited paragraphs state that the problems of the prior art *can* be addressed by a database update...[but that] there is no specific solution stated in the cited paragraphs."

Applicant respectfully disagrees with such arguments. Applicant emphasizes the following language from paragraph [0005] which states "[t]his inflexibility can be addressed by updating the database of the KDC; however, since the KDC can itself be a wireless node, and perhaps a mobile node, this update is expensive both in terms of energy and bandwidth." In addition, in paragraph [0006] applicant states that "[w]hat is needed is a method...that provides for establishing shared cryptographic keys between participating nodes without the difficulties listed above."

Thus, clearly applicant's specification discloses that a technique is needed other than updating when the KDC is a wireless node or a mobile node. Furthermore, applicant points out paragraph [0033] which states that the key distribution center "can include mobile secure communication devices." Since applicant specifically describes a KDC being a mobile device [0033], that a KDC as a mobile node would result in expansive energy and bandwidth when using updates [0005], and that a method is needed that provides for establishing shared cryptographic keys between participating nodes without such difficulties [0006], applicant respectfully asserts that clearly "wherein an update of a

key distribution center database of shared keys is, at least in part, capable of being avoided when at least one of the nodes is unfamiliar" is not merely a possibility as the Examiner contends. Instead, the remaining parts of the specification clearly describe an exemplary associated solution.

The Examiner has rejected Claims 1, 3-18 and 20 under 35 U.S.C. 112, second paragraph as being indefinite. The Examiner has argued that applicant's claimed technique "wherein an update of a key distribution center database of shared keys is, at least in part, capable of being avoided when at least one of the nodes is unfamiliar" (see each of the independent claims) is unclear. Applicant respectfully asserts that such rejection is avoided by virtue of the clarifications made to the claims hereinabove.

Still with respect to each of the independent claims, the Examiner has also stated that it is not clear whether the verifications in applicant's claimed "verifying the hash value" take place at the first node, the second node, or the key distribution center. In the latest Office Action dated 9/20/2005, the Examiner has first argued that it was originally claimed at which node the hash value verifications take place. Applicant respectfully asserts that such limiting language was removed from the claim to provide for the hash value to be verified at the first node and/or second, thus providing claim breadth.

The Examiner has secondly argued that removal of specific node locations for the hash verification raises further issues of indefiniteness for Claims 8 and 11. Applicant has clarified Claim 8 to overcome such indefiniteness.

The Examiner has thirdly argued that "in light of applicant's specification, it is clear that one of the hash verifications takes place at a first node and the other verification at the second node, and that the locations of these verifications are vital to the functioning of the claimed protocol." Applicant respectfully asserts that Figure 6 does not include operations for validating hash values, as the Examiner has contended, but that instead Figure 6 only shows decrypting a shared key at a second node/first node (operations 616 and 622) and creating proof of having the shared key at the second node/first node

(operations 618 and 626). However, as described in the specification, between operations 616/622 and 618/626, a hash validator may validate the shared key (see page 15, paragraphs [0061] and [0063]). Simply nowhere does applicant describe that such verifications are "vital" as the Examiner argues. In fact, in view of the omission of such claimed subject matter in Figure 6, applicant respectfully asserts that such verifications are not vital as argued by the Examiner.

Applicant emphasizes that "[i] n determining whether an unclaimed feature is critical, the entire disclosure must be considered. Features which are merely preferred are not to be considered critical." In re Goffe, 542 F.2d 564, 567, 191 USPQ 429, 431 (CCPA 1976). In re Mayhew, 527 F.2d 1229, 1233, 188 USPQ 356, 358 (CCPA 1976).

Further, limiting an applicant to disclosed features in the absence of limiting prior art would not serve the constitutional purpose of promoting the progress in the useful arts. Therefore, a rejection based on the grounds that a disclosed critical limitation is missing from a claim should be made only when the language of the specification makes it clear that the limitation is critical for the invention to function as intended. Broad language in the disclosure, including the abstract, omitting an allegedly critical feature, tends to rebut the argument of criticality. See MPEP 2164.08(c). In the present case, there is no discussion of elements deemed critical in the specification. Further, it should be noted that there are no such elements in the Abstract, as filed.

The Examiner has rejected Claims 1-21 under 35 U.S.C. 103(a) as being unpatentable over Menezes et al., *Handbook of Applied Cryptography*. Applicant respectfully disagrees with such rejection.

The Examiner has persisted with the current rejection. As set forth below, such rejection is still deficient. However, despite such deficiencies and in the spirit of expediting the prosecution of the present application, applicant has incorporated the subject matter of dependent Claims 3-7 into each of the independent claims.

With respect to each of the independent claims, the Examiner has relied on page 503, protocol 12.26, message 1 of Menezes to make a prior art showing of applicant's claimed "sending a first message from the first node to the second node, wherein the first message requests establishing the cryptographic key." Applicant respectfully asserts that Menezes teaches that "A interacts with trusted server T and party B" and that the result is entity authentication between A and B (see page 503, 12.26). There is simply no disclosure of a "first message [that] requests establishing the cryptographic key," as claimed by applicant (emphasis added). Instead, Menezes only generally teaches that entity authentication is established from A's interaction with T and B.

In the latest Office Action dated 9/20/2005, the Examiner has responded to such arguments by stating that Menezes teaches key establishment. However, applicant notes that Menezes only generally teaches "key establishment with key confirmation" (see page 503 Protocol 12.26 "Result"), but not that a first message from a first node "requests establishing the cryptographic key" as specifically claimed by applicant (emphasis added). Furthermore, message 1 in protocol 12.26 on page 503, as relied on by the Examiner, only shows a message from A to T (server). Clearly, a message from node A to server T does not meet applicant's specifically claimed "sending a first message from the first node to the second node," and especially not when read in context, as argued above (emphasis added).

The Examiner has also relied on page 503, protocol 12.26, message 1 of Menezes to meet applicant's claimed "sending a second message from the second node to a key distribution center, wherein the second message includes a first node identifier for the first node, [and] a second identifier for the second node...". Applicant respectfully asserts that Menezes only generally teaches entity authentication between A and B as a result of A interacting with T and B. Such teaching does not meet applicant's specific claim language since there is no mention of any sort of second message from the second node to a key distribution center. In fact, Menezes discloses that T chooses the session key such that there would be no need for a second message in the manner claimed by

applicant and in addition there is clearly not even a suggestion of any sort of "key distribution center," as claimed by applicant.

In the latest Office Action dated 9/20/2005, the Examiner has failed to respond to applicant's arguments that Menezes does not teach "sending a second message from the second node to a key distribution center." Applicant argues that the only messages sent from the second node (B), as disclosed in protocol 12.26, are sent to the first node (A). Menezes only teaches that node A sends a message to server T, and not that "a second message [is sent] from the second node to a key distribution center" as claimed by applicant (emphasis added).

Further, the Examiner has admitted that Menezes does not explicitly disclose applicant's claimed "message authentication code created using a second node key belonging to the second node" and "recreating the second node key at the key distribution center, wherein the second node key was previously created using the second node identifier and a secret key known only to the key distribution center."

To meet such language, the Examiner has responded to applicant's arguments by stating that Menezes discloses MAC's (page 361, below definition 9.77) and identity-based keying (page 561, section 13.4.3), and that it would have been obvious to modify the key distribution protocol by including the use of a MAC in order to provide data origin authentication and data integrity, and by including identity based keying in order to prevent forgery and impersonation.

Applicant respectfully disagrees with the Examiner's assertion. Specifically, Menezes simply teaches that one way, out of three possible ways, for providing data origin authentication is carried out by way of MAC's. Such a general disclosure of why MAC's are used simply does not meet applicant's specific claim language. Particularly, there is simply no suggestion in Menezes of any sort of second message that is sent from a second node to a key distribution center, where the second message includes a MAC.

Menezes teaches utilizing MAC's between parties sharing a key, and not between a second node and a key distribution center.

In addition, Menezes does not disclose that the MAC is "created using a second node key belonging to the second node," as claimed by applicant. Menezes simply teaches that the MAC is the shared key, but not that it is created by a key belonging to one of the parties.

In the latest Office Action dated 9/20/2005, the Examiner has first stated that applicant's arguments are spurious, "as the second node and the key distribution center, as claimed, share a key (i.e. the second node key)." However, nowhere does applicant claim that the second node and that key distribution center share a key, as the Examiner seems to contend. Instead, applicant claims "recreating the second node key at the key distribution center...using...a secret key known only to the key distribution center" (emphasis added).

In the latest Office Action dated 9/20/2005, the Examiner has secondly stated that "Menezes states that MACs are *based on* secret shared keys (see page 361, below definition 9.77)." Applicant respectfully disagrees, and notes Menezes' explicit language that "[d]ata origin authentication mechanisms [are] based on shared secret keys (e.g. MACs)" (emphasis added). Thus, Menezes expressly discloses that MACs are an example of a shared secret key, and not that a MAC is "created using a second node key belonging to the second node" as specifically claimed by applicant (emphasis added). The Examiner has further relied on page 352, section 9.5 and page 353, algorithm 9.58 in Menezes in arguing that Menezes teaches that a MAC is created by a secret encryption key. Applicant respectfully asserts that section 9.5 on page 352 does not even suggest any sort of "secret encryption key" as argued by the Examiner. Furthermore, the algorithm on page 353 only generally discloses a "secret key," but not where such secret key comes from, and especially not that the MAC is created using "a second node key belonging to the second node" as claimed by applicant.

Still with respect to each of the independent claims, applicant respectfully emphasizes that the Examiner admits that the protocol in Menezes "does not explicitly disclose recreating a first node key previously created using the first node identifier and the secret key." The Examiner goes on to argue that "Menezes discloses identity-based keying" and further "although the protocol does not explicitly disclose the use of a hash value in the messages for verification, Menezes discloses that hash values can be used for verification of data." The Examiner then concludes that "it would have been obvious to one of ordinary skill in the art at the time the invention was made to further modify the key distribution protocol by including the use of a hash, in order to provide data integrity." Applicant emphasizes the arguments made hereinabove which clearly show that it would not have been obvious to modify Menezes as suggested by the Examiner since Menezes is still deficient in many respects.

The Examiner has responded by further arguing that "the fact that applicant has recognized other advantages which would flow naturally from following the suggestion of the prior art cannot be the basis for patentability when the differences would otherwise be obvious." Applicant respectfully asserts that the claimed advantages would not flow naturally and also that the difference would not be obvious.

Specifically, applicant previously noted in paragraph [0005] of the originally filed specification that applicant's claimed invention provides a particular advantage over key distribution schemes such as Kerberos in that database updates are not required for unfamiliar participants. Since the technique relied upon by Menezes is analogous to Kerberos, it explicitly lacks, and even *teaches away* from, any sort of similar advantage and thus could not flow naturally from the prior art. For these reasons, applicant contends that it would simply not be obvious to modify Menezes to meet applicant's claim limitations noted above.

In the latest Office Action dated 9/20/2005, the Examiner has again responded to applicant's arguments by stating that the amendment made previously with respect to each of the independent claims fails to comply with 37 CFR 1.111(b) since it amounts to

a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.

Applicant again respectfully points out that, in applicant's claimed invention, database updates are at least partially not required for unfamiliar participants. Since the technique relied upon by Menezes is analogous to Kerberos, it explicitly lacks, and even *teaches away* from, not requiring database updates for unfamiliar participants. To emphasize, applicant asserts that Menezes lacks any disclosure of not requiring database updates for unfamiliar participants, and therefore would not provide any sort of obvious basis for rejecting applicants specific claim language.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the first and third element of the *prima facie* case of obviousness have not been met, since the prior art reference fails to teach or suggest all the claim limitations, and it would not be obvious to modify the prior art reference, as suggested by the Examiner. Nevertheless, despite such paramount deficiencies and in the spirit of expediting the prosecution of the present application, applicant has substantially incorporated the subject matter of Claims 3-7 into each of the independent claims.

With respect to the subject matter of Claim 3, the Examiner has relied on page 503, protocol 12.26, message 1 in Menezes to make a prior art showing of applicant's claimed technique "wherein the first message includes the first node identifier, the second node identifier, a third identifier for the key distribution center, and a first nonce, wherein a nonce is a random number selected for message confirmation purposes that has a statistically low probability of being reused." However, applicant notes that message 1 only discloses a message that is sent from node A to server T. Clearly a message that is sent between node A and server T does not meet applicant's claimed "first message" since, when read in context, applicant's "first message" is sent from a first node to a second node. Furthermore, the only information included in message 1 is A, B and N_A, and not "a third identifier for the key distribution center" as specifically claimed by applicant.

With respect to the subject matter of Claim 4, the Examiner has again relied on page 503, protocol 12.26, message 1 in Menezes to make a prior art showing of applicant's claimed technique "wherein the second message includes the third identifier, the second node identifier, the first node identifier, a second nonce, the first nonce, and the message authentication code, wherein the message authentication code is created from the third identifier, the second node identifier, the first node identifier, the second nonce, and the first nonce."

First, applicant respectfully asserts that message 1, as relied on by the Examiner, only discloses a message that is sent from node A to server T. Clearly a message that is sent between node A and server T does not meet applicant's claimed "second message" since, when read in context, applicant's second message is sent from a second node to a key distribution center, and not a first node as shown by Menezes. Second, the only information included in message 1 is A, B and N_A, and not "the third identifier... a second nonce...and the message authentication code, wherein the message authentication code is created from the third identifier, the second node identifier, the first node identifier, the second nonce, and the first nonce" as specifically claimed by applicant.

With respect to the subject matter of Claim 5, the Examiner has relied on pages 321-322, section 9.1 in Menezes to make a prior art showing of applicant's claimed technique "wherein verifying the message authentication code includes: creating a test message authentication code from the third identifier, the second node identifier, the first node identifier, the second nonce, and the first nonce using the second node key; and comparing the test message authentication code with the message authentication code."

Applicant respectfully asserts that such excerpt merely relates to creating a hash of a message to determine later on if such message has been altered (i.e. by comparing such original hash to a subsequent hash of the message created later on). However, Menezes only generally discloses the hash, which clearly fails to meet applicant's specific claim language, namely that a "test message authentication code [is created from] the third identifier, the second node identifier, the first node identifier, the second nonce, and the first nonce using the second node key" (emphasis added).

With respect to the subject matter of Claim 6, the Examiner has relied on page 322, first full paragraph, in Menezes to make a prior art showing of applicant's claimed technique "wherein the hash value is created from the second node identifier, the first node identifier, the second nonce, and the first nonce." Again, applicant respectfully asserts that Menezes only generally discloses a hash, but not specifically that a "hash value is created from the second node identifier, the first node identifier, the second nonce, and the first nonce" as claimed by applicant.

With respect to the subject matter of Claim 7, the Examiner has relied on page 503, protocol 12.26, message 2, to make a prior art showing of applicant's claimed technique "wherein the third message includes the second node identifier, the first node identifier, the second encrypted key, and the first encrypted key." Applicant respectfully asserts that such message as relied on by the Examiner is with regard to a message from the server T to the node A. However, applicant's claimed "third message" is, when read in context, sent "from the key distribution center to the second node." Clearly a message sent from a server to a first node does not meet applicant's claimed third message that is

sent from a key distribution center to a second node, especially since applicant's claimed second node has functionality that is at least partially different from applicant's claimed first node.

Applicant respectfully asserts that at least the first and third element of the *prima facie* case of obviousness have not been met, since the prior art reference fails to teach or suggest all the claim limitations, and it would not be obvious to modify the prior art reference, as noted above.

Applicant further notes that the prior art is also deficient with respect to the dependent claims. Just by way of example, with respect to Claim 8, the Examiner has again relied on the first full paragraph on page 322 in Menezes to make a prior art showing of applicant's claimed technique "wherein validating the hash value at the second node includes: creating a first test hash value from the second node identifier, the first node identifier, the second nonce, and the first nonce; and comparing the first test hash value with the hash value." Yet again, applicant respectfully asserts that Menezes only generally discloses a hash, but not specifically that a "first test hash value [is created] from the second node identifier, the first node identifier, the second nonce, and the first nonce" as specifically claimed by applicant (emphasis added).

With respect to Claim 9, the Examiner has relied on page 503, protocol 12.26, message 5 in Menezes to make a prior art showing of applicant's claimed technique "wherein the fourth message includes the first node identifier, the second node identifier, the second nonce, the first encrypted key, and a first confirmation value, wherein the first confirmation value has been encrypted with the cryptographic key." Applicant respectfully asserts that such message only includes the encryption key and the second nonce, and not "the first node identifier, the second node identifier... and a first confirmation value, wherein the first confirmation value has been encrypted with the cryptographic key" as specifically claimed by applicant (emphasis added).

With respect to Claim 10, the Examiner has again relied on page 503, protocol 12.26, message 5 in Menezes to make a prior art showing of applicant's claimed technique "wherein the first confirmation value includes the second nonce and the first nonce." Applicant respectfully asserts that message 5, as relied on by the Examiner, only includes the encryption key and the second nonce, but not any sort of confirmation value, let alone where such confirmation value "includes the second nonce and the first nonce" as specifically claimed by applicant.

With respect to Claim 11, the Examiner has relied on the first full paragraph on page 322 in Menezes to make a prior art showing of applicant's claimed technique "verifying the hash value includes: creating a second test hash value from the second node identifier, the first node identifier, the second nonce, and the first nonce; and comparing the second test hash value with the hash value." Applicant respectfully asserts that such excerpt only generally discloses a hash, but not specifically that a "second test hash value [is created] from the second node identifier, the first node identifier, the second nonce, and the first nonce" as claimed by applicant (emphasis added).

With respect to Claim 13, the Examiner has relied on page 503, protocol 12.26, message 4 in Menezes to make a prior art showing of applicant's claimed technique "wherein the fifth message includes: the second node identifier, the first node identifier, and a second confirmation value." Applicant respectfully asserts that message 4 in Menezes only includes an encryption key and a second nonce, and not the "second node identifier, the first node identifier, and a second confirmation value" as specifically claimed by applicant. Furthermore, message 4 in Menezes is sent from the second node (B) to the first node (A), which clearly does not meet applicant's "fifth message" since applicant's fifth message is sent from the first node to the second node "so that the second node can confirm that the cryptographic key has been established" (see independent claims).

With respect to Claim 14, the Examiner has again relied on page 503, protocol 12.26, message 4 in Menezes to make a prior art showing of applicant's claimed

technique "wherein creating the second confirmation value at the first node includes: reordering the first nonce and the second nonce recovered by decrypting the first confirmation value to create the second confirmation value; and encrypting the second confirmation value using the cryptographic key." Applicant respectfully asserts that such message only includes a encryption key for encrypting a second nonce, and does not even suggest "reordering the first nonce and the second nonce recovered by decrypting the first confirmation value to create the second confirmation value; and encrypting the second confirmation value using the cryptographic key" as specifically claimed by applicant (emphasis added).

Again, applicant respectfully asserts that at least the first and third element of the *prima facie* case of obviousness have not been met, since the prior art reference fails to teach or suggest all the claim limitations, and it would not be obvious to modify the prior art reference, as noted above.

A notice of allowance or a specific prior art showing of each of the foregoing limitations, in combination with the remaining claim elements, is respectfully requested.

To this end, all of the pending independent claims are deemed allowable, along with any dependent claims dependent therefrom.

Reconsideration is respectfully requested.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. Applicants are enclosing a check to pay for the added claims. The Commissioner is authorized to charge

any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P254/01.001.01).

Respectfully submitted,
Zilka-Kotab, PC

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100